Fortiweb Troubleshooting

Rajashekar Reddy – Technical Support Engineer

FortiGuard Connectivity and Registration Issues (1/2)

- Ensure that the time zone set on the FortWeb unit is correct.
- Check if FortiWeb is allowed to access the Internet on TCP port 443 and ICMP (this is for connectivity test purposes) and DNS(UDP 53. If the defined DNS server is on the internet).
- Test connectivity to the FortiGuard servers by executing the following commands:

  execute ping service.fortiguard.net

  execute ping update.fortiguard.net
- If the resolution to FortiGuard servers fails, verify the DNS configuration
- If the ping to FDS servers is successful, but the problem still persists, run the following commands for additional information:

  diagnose debug reset

  diagnose debug application fds 7

  diagnose debug enable

  execute update-now

FortiGuard Connectivity and Registration Issues (2/2)

- Additionally, enable packet capture to the FDS server IP found in the debug output as a result of running commands in the previous step.

Reverse Proxy Mode

- Requests are destined for a virtual server's network interface and IP address on FortiWeb, not a web server directly.
- FortiWeb finds the matching server policy by looking up the destination IP address and the destination port in the received SYN packet from the client against the defined server policies.
- By default, FortiWeb uses the interface IP address to communicate with the real server.
- Fortiweb parses only HTTP(S)/FTP(S). Parsed data will be scanned against the protection profile applied to the server policy.
- FortiWeb doesn't forward non-HTTP(S)/FTP(S) traffic to the protected real server(s). Need to Enable IP forwarding in CLI to route them to the real server(s)

```
config router setting
 set ip-forward {enable | disable}
end
```

True Transparent Proxy(TTP) & Transparent Inspection(TI)

- TTP: FortiWeb transparently proxies the traffic arriving on a network port that belongs to a Layer 2 bridge, FortiWeb logs, blocks, or modifies violations according to the matching policy and its protection profile.
- TI: FortiWeb asynchronously inspects traffic arriving on a network port that belongs to a Layer 2 bridge, applies the first applicable policy, and lets permitted traffic pass through. (Because it is asynchronous, it minimizes latency.) FortiWeb logs or blocks traffic according to the matching policy and its protection profile, but does not otherwise modify it. (It cannot, for example, offload SSL, load-balance connections, or support user authentication.

Offline Protection Mode

- Requests are destined for a web server, not the FortiWeb appliance. Traffic is duplicated from the flow and sent on an out-of-line link to the FortiWeb through a switched port analyzer (SPAN or mirroring) port.

- Unlike in Reverse Proxy mode or True Transparent Proxy mode, actions other than Alert cannot be guaranteed to be successful in Offline Protection mode.

- “Out-of-band” is an appropriate descriptor for this mode. Minimal changes are required. It does not introduce any latency. However, many features are not supported

High Availability (1/4)

- physical connection: monitor port peers should in the same subnet.
- physical connection: heartbeat port peers should connect each other between 2 FWBs with a cross line.
- configuration: 2 FWB ha peers should have the same unique group id, and should not same as another ha group.
- configuration: use different priority on 2 FWB ha peers and enable override, will keep high priority one (with a smaller value) on the main role as much as possible.
- command: 'get system status' or 'get global system status', show current HA members' information which includes HA mode/HA Status/Serial-Number/priority/HA-Role. It can help us to confirm if the 2 peers working in the same HA group and which one is the Primary.
- command: 'exe ha md5sum', get CLI/System configuration MD5 from 2 HA peers. It helps us to confirm if the HA configuration is in sync or not

High Availability (2/4)

- command: 'exe ha disconnect', should run on main. It can disconnect slave one to a new management ip.
- command: 'exe ha manage', should run on main. It can change slave one priority, in other word, if override enabled, it can trigger HA failover manually.
- command: 'exe ha synchronize config/waf/irdb', trigger configuration synchronization manually. These 3 parts of configuration can be auto sync to HA peer. This command also can refresh md5sum value, in order to confirm the configuration sync status.
- command: 'exe ha synchronize avupd/geodb', trigger 2 database file synchronization manually. These 2 parts of file sync won't auto sync to HA peer, have to manually trigger sync.
- command: 'exe ha synchronize start/stop', start/stop sync during configuration debugging.

High Availability (3/4)

- diagnose: 'diag debug app hasync 7', get debugging info during ha sync configuration. Should run it on both console of 2 HA peers to confirm the configuration sync and communication. It shows us auto configuration sync process, which command failed and what happened during full configuration sync
- diagnose: 'diag debug app hatalk 7', get debugging info of ha heartbeat related. It shows us if heartbeat exist and how ha failover, also can get lifetime of ha peers.
- Debug HA INIT:
- Bring the slave unit on network and make sure the slave unit shows in “INIT” mode on the master unit GUI.
- Once you have slave unit in INIT mode, run the following commands on the master unit and get the files as explained below

  diagnose system ha sync-config set-status disable

  diagnose system ha backup-config 1

  diagnose system ha backup-config 2

High Availability Debug (4/4)

- Enable GUI file upload:

  config global

  config system settings

  set enable-file-upload enable

  end
- Download the two backup files from System->Maintenance->Backup&Restore in GUI

CPU and Memory Troubleshooting (1/2)

- Does CPU usage spike during a specific time of the day?
- Does some process keep running into crashes?
- Useful Commands

  diagnose system top <-----leave for a minute.

  get system performance<------please take it for 40 sec.

  diagnose debug crashlog show

  diagnose hardware mem list

  diagnose hardware cpu list

  diagnose policy memory all

  diagnose policy total-conn-psec list

  diagnose policy total-session list

  diagnose policy total-traffic list

  diagnose policy total-traffic http list

CPU and Memory Troubleshooting (2/2)

- diagnose policy conn-psec list root.<server policy name>
- diagnose policy session list root.<server policy name>
- diagnose policy traffic list root.<server policy name>
- diagnose hardware cp9 status
- diagnose system top
- diagnose system perf

URL Rewriting and Redirection (1/3)

- Request Action rewrites HTTP requests from Client, and Response Action Rewrites responses to clients from the web server.

URL Rewriting and Redirection can be applied in the following scenarios:

- Redirect HTTP requests to HTTPS
- Rewrite the URL line in the header of an HTTP request
- Rewrite the Host: field in the header of an HTTP request
- Rewrite the Referer: field in the header of an HTTP request
- Redirect requests to another website.
- Send a 403 Forbidden response to matching HTTP Requests.
- Rewrite The HTTP location line in the header of matching redirection response from the web server.
- Rewrite the body of an HTTP response from the web server.

URL Rewriting and Redirection (2/3)

- Response rewrite rule and the action is “Rewrite HTTP Body” ensure there is a Content-Type header in the response from the backend server and the content-type must be supported by the Fortiweb:

FortiWeb supports the following Content-Type values only:

- text/html
- text/plain
- text/javascript
- application/xml
- text/xml
- application/javascript
- application/soap+xml
- application/x-javascript
- application/json & application/rss+xml

URL Rewriting and Redirection (3/3)

- HTTP to HTTPS Redirect: This rewriting rule has 3 parts:
  - Regular expression that matches HTTP requests with any host name—(.*)
  - Regular expression that matches requests with any URL in the HTTP header—^/(.*)$.
  - Redirect destination location that assembles the host name ($0) and URL ($1) from the request in front of the new protocol prefix, https://

Content Routing

- Content Routing policies define how fortiweb routes requests to server pools, Below are the following HTTP elements:
  - Host
  - URL
  - HTTP Parameter
  - Referer
  - Source IP
  - Header
  - Cookie
  - HTTP SNI
  - X509 Certificate Field value

Certificates

- SSL offloading or SSL inspection—Server certificates do not belong to the FortiWeb appliance itself, but instead belong to the protected web servers.
- FortiWeb uses the web server's certificate because it either acts as an SSL agent for the web server.
- If a server certificate is signed by an intermediate certificate authority (CA) rather than a root CA, before clients will trust the server certificate, you must demonstrate a link with root CAs that the clients trust.
- In some cases, servers host multiple secure websites that use a different certificate for each host. To allow FortiWeb to present the appropriate certificate for SSL offloading, you create an inline or offline Server Name Indication (SNI).
- SSL termination cannot be supported in Transparent Inspection and Offline Protection In those modes, the webserver uses its own certificate, and acts as its own SSL terminator.

Web Protection (1/2)

- If FortiWeb is identifying legitimate requests as attacks (false positives), complete the following troubleshooting steps:

- If your web protection profile uses a signature policy in which the extended version of a signature set is enabled Example: Cross Site Scripting disable it. The extended signature sets detect a wider range of attacks but are also more likely to generate false Positives.
- Specify the appropriate URL as an exception in the signature configuration. To create this exception, click either the Exception link in the Message field of the attack log item or Advanced Mode in the Edit Signature Policy dialog box.
- If the configuration changes do not solve the problem, capture the packet that FortiWeb has incorrectly identified as an attack and contact Fortinet Technical Support for assistance. Fortinet can resolve the issue by modifying the attack signature.

Web Protection (2/2)

- If FortiWeb is identifying attacks as legitimate requests (false negatives), complete the following troubleshooting Steps:

- Use the Advanced Mode option to ensure that the signature policy that your web protection profile uses has the following configuration:
- All the appropriate signatures are enabled.
- The enabled signatures do not have exceptions that permit the attack packets.
- If your signature configuration is correct, capture the packet that FortiWeb did not identify as an attack and contact Fortinet Technical Support for assistance.
- In the meantime, you can resolve the problem by creating a custom signature.

URL Access Rule

- Why a URL access rule doesn’t work?

- The URL Pattern value in a URL access rule shouldn’t include the parameter part. That is to say that the value here only matches against the URL string before the question mark.
- URL access rules may be skipped by previous rule if previous rule has been matched because all of the rules are checked by their sequences.

MITB

- Why doesn't MITB work?

- Make sure the request URL matches that rule and the response page is in HTML format with status code 200.
- Make sure there’s a form tag in the response HTML page and the form’s action URL matches the POST URL in MITB rule.
- Make sure the type of password input tag is “password” indeed, or FortiWeb’s MITB script can’t locate the password.
- Make sure the value of the Content Security Policy header doesn’t block the execution of FortiWeb's MITB script.

Logging (1/5)

- Check if log options are enabled correctly:

Make sure global log options are enabled via GUI or CLI as below:

FortiWeb # show full log event-log

config log event-log

set status enable

end

FortiWeb # show full log traffic-log (Attack-log)

config log traffic-log

set status enable

end

Logging (2/5)

- Log disk is "Not available", it means the log disk file system is damaged or hardware damaged.
- Below CLI command to recreate the log disk file system
- execute formatlogdisk
- If it works fine you can rebuild the database.
- execute db rebuild
- Check the disk usage. Make sure that the disk usage is not full
- diag system mount list

Logging (3/5)

- Do you see the logs being written here?
- cat /var/log/fwlog/root/disklog/tlog.log (shell command)
- Collect outputs below:
- /# cat /var/log/dlog_logd (shell command)
- /# cat /var/log/dlog_indexd (shell command)
- Debug commands to show info:
- diagnose debug application sysmon 7
- diag debug application logd 7
- diag debug enable

Logging (4/5)

- 7.0.0 and later releases, traffic log is disabled by default and can be enabled or disabled per server-policy policy via CLI:

```
FortiWeb # show full-configuration server-policy policy
    config server-policy policy
    edit "SP_01"
    set tlog enable
    end
```

- Logging Issues:

-Check if logd, indexd and mysqld work normally.

```
ps | grep logd
ps | grep indexd
ps | grep mysqld
```

Logging (5/5)

- Diagnose commands to check the logds outputs:
  - diagnose debug application logd 7
  - diagnose debug timestamp enable
  - diagnose debug enable
- Find the root cause via more detailed backend logs or counters:
  - cat /var/log/dlog_indexd.
  - tail -f /var/log/dlog_indexd
  - cat /var/log/dlog_indexd | grep mysql
  - cat /var/log/mysql/error.log
  - cat /var/log/fwlog/root/disklog


FORTINET